==
HIPAALERT -- Volume 3, Number 11 - December 3, 2002

>>From Phoenix Health Systems--HIPAA Knowledge--HIPAA Solutions<<
=>Healthcare IT Consulting & Outsourcing<=
==
HIPAAlert is published monthly in support of the healthcare industry's efforts to work together towards HIPAA security and privacy. Direct subscribers total almost 20,000.

==

THIS ISSUE

==

==

1 >> FROM THE EDITORS:

As winter approaches, many organizations covered by HIPAA regulations are well along in gap assessment and HIPAA awareness efforts, but at least half (based on our most recent industry survey results) have either not begun actual remediation or are still in planning stages. (See the November special survey edition of HIPAAlert available at HIPAAdvisory.com.) Because implementation costs remain a major concern, this HIPAAlert leads off with a recommended, detailed approach for costing out an enterprise-wide HIPAA implementation. Excerpted from a column we recently wrote for Health Management Technology magazine, it hopefully will help you get "from here to there" by mid-April - the deadline for Privacy compliance and readiness for transactions testing.

Other offerings this month focus on security compliance, including an informative discussion of data backup approaches by guest contributor Jenny Pemberton, and an analysis of access control applicability to HIPAA by Eric Maiwald. Finally, Steve Fox and Rachel Wilson explore how and when assisted living facilities are covered by HIPAA regulations.

D'Arcy Guerin Gue, Publisher
dgue@phoenixhealth.com

Bruce Hall,
Director of Internet Services
bhall@phoenixhealth.com

==

==

2 >> HIPAAnews

** Simpler Final Security Rule to Harmonize with Privacy **

According to Dr. William Braithwaite, the final security rule due out December 27 will be more harmonized with the Privacy Rule. Braithwaite, national director of HIPAA advisory services at PricewaterhouseCoopers, and former senior advisor on health information policy for HHS, noted the following likely changes in the final rule, during comments at last month's HIPAA Summit in Baltimore:

* The rule requirements will be clarified and redundancies removed. Chain of trust agreements will be necessary in business associate agreements, but not in agreements with other covered entities.

* The final rule will follow the same philosophy as the proposed rule, only applying to electronically maintained and transmitted health information. It will continue to be technology neutral. Secure encryption technology will be required when transferring protected health information (PHI) specifically across the internet or automated clearinghouse networks.

* There will be no electronic signature standard, though HHS may later release a separate rule for electronic signatures.

** Federal Agencies Flunk Security Final Exam **

Federal agencies overall earned an "F" on Rep. Stephen Horn's latest report card on government security -- the same grade they earned in 2001. When he issued his first computer security report card in 2000, Horn (R-CA), a former professor and president of California State University at Long Beach, awarded agencies an overall grade of D-. The Department of Health and Human Services received a grade of D-; the highest grade was a B-minus.

Read more: http://www.hipaadvisory.com/news/index.cfm#1120fcw

** Homeland Security vs. Personal Privacy **

Civil libertarians have warned that the homeland security bill passed by Congress and the Senate, taken in context with broadened surveillance powers and new database technology, represents an unprecedented threat to personal privacy. The Senate has voted overwhelmingly to create a new Homeland Security Department after the House passed a nearly identical version of the bill last week. A major area of contention involved permitting the department to develop a Total Information Awareness program that will sift through electronic data, such as medical records, in search of possible terror plots.

Read more: http://www.hipaadvisory.com/news/2002/1120usapatriot.htm

** Revised Summaries of Remaining State Health Privacy
Laws Released **

Last week, the Health Privacy Project released the final batch of revised summaries of the health privacy statutes of the remaining six states: Maine, North Carolina, Ohio, Tennessee, West Virginia and Wisconsin. These updated summaries reflect changes in state health privacy statutes that have been made since the original report, "The State of Health Privacy: An Uneven Terrain," was published in 1999. The 1999 version of the report will be available until the full 2002 updated edition is available, which will be posted on the Health Privacy Project's web site later this month.

===

http://www.hipaadvisory.com/wares/HIPAAbook.htm

==

3 >> HIPAAction: Feature Article

** What Is HIPAAffordable:
Costing Out Your HIPAA Implementation Project **

By D'Arcy Guerin Gue (with John Spearly and Tom Grove)

Depending on your politics, assessments of the costs to America's healthcare industry for HIPAA implementation range from reasonable (including ROI factors), to ruinous. The proverbial jury is still out.

What should you be spending? How should you cost out your organization's HIPAA implementation expenditures -- and what will be cost effective, at the very least -- and possibly even beneficial to your operations? Are there proven models you can work from so that HIPAA will not end up simply a major organizational brain- and dollar-drain?

Unlike healthcare organizations that have more things to worry about (such as healthcare delivery), expert HIPAA consultants have been able to justify drilling down into these issues for years. But you don't have to hire a consultant to take advantage of their costing methodologies. Consider the following proven costing model:

ASSUMPTIONS - INTERNAL COSTS

Unless you have staff with no other work to do, start by recognizing that internal work efforts have a real dollar cost. Simplify your staff costs for HIPAA work to a few levels (rather than in precise detail) to minimize calculation complexities. Real client examples suggest that the time of physicians and senior executives should be calculated at $100 per hour, management staff at $35 per hour and other staff at $25. If these numbers seem high, recognize that they are "loaded" rates that include indirect (i.e. benefits) and overhead costs. If these numbers still seem high for your organization, create your own; the point is, don't exclude them because the staff is already in place -- and be realistic in designating appropriate cost figures.

ASSUMPTIONS - EXTERNAL COSTS

No surprises here. External costs for management and technical consulting support will likely be the single biggest line item cost outside of technical security purchases. On the other hand, with careful planning, they may represent the highest value dollars you spend, depending on your staff's level of expertise and available time -- and considering the learning curve they may have to get the job done. Expect to pay $150 - $300 per hour plus expenses for qualified management consultants, and between $125 and $225 per hour for technical consultants. Where used, consultants should be part of an internal-external mix, rather than hired to "make us compliant." Without equal or great internal staff involvement, costs will be exorbitant, knowledge transfer low, and results undoubtedly poor.

MAJOR INITIATIVES

Now consider what must be done. Necessary implementation tasks (which should have been generated through your gap analysis) and associated costs include:

----
* Project Management:

The primary cost driver is hours allocated for project manager and staff. For large hospitals, systems, payers and clearinghouses, a full time effort is required to manage the HIPAA implementation project. For mid-size hospitals, at least 16 hours per week should be allocated -- plus strong support. For small facilities, allocate at least 12 hours per week until the project is complete. Then, apply appropriate hourly.

Tip: Actual hours required will depend heavily on support provided to the Project Manager by other staff.

----
* Data Flow Analysis:

This effort, required by the Security NPRM, will be invaluable for understanding the effects of identifiers throughout your information systems and for developing effective privacy practices. Primary cost driver is the number of peer to peer connection points within the organization. Focus should be on three major areas: internal electronic data flow, external electronic data flow, and both internal and external paper flow. Once you know the total number of connection points, multiply them by your estimate of the number of minutes or hours required to identify and document findings. For example, a small hospital's internal paper data flow analysis might indicate 12 departments X 4 hours each, and 28 unique reports X 2 hours each -- for a total of 100 hours. Large hospitals are likely to end up with a cost of $150,000 or more, mid-size hospitals $75,000, and small hospitals $25,000.

----
* Risk Management:

Primary cost drivers: cost of staff to manage the process, and cost of a new risk-tracking system. Program development efforts will create the need to front load this effort. Large entities are likely to spend half-time effort of one person for six weeks -- with four hours per week thereafter. These numbers will be halved for mid-size organizations, and could be closer to five hours per week for the first six weeks, with one hour per week thereafter for small facilities.

----
* Vendor Management:

This effort will include vendors of software systems that include protected health information (PHI), payers and clearinghouses. Cost drivers include number of critical vendors; hours estimated, per vendor, to track their compliance efforts, and consulting assistance, if needed.

Tip: Include time to collect data, make repeated contact attempts, and analyze results. Large facilities may need to consider a document management tool. Cost out by multiplying the number of vendors of each type by the number of hours needed to address each vendor. Major software vendors and clearinghouses will require 8-16 hours each; minor vendors about half this number.

----
* Upgrade Systems:

While most vendors will provide free upgrades (if you have appropriate maintenance programs in place), you still must consider costs including developing a new infrastructure, consulting assistance, training and testing. Cost drivers include number of critical vendors identified, hours estimated per vendor to track compliance efforts, and consulting assistance. Costs should be calculated on a per system basis.

----
* Transaction Testing:

All organizations should consider formal testing of transaction output, especially for self-developed transactions systems. At least one major commercial testing vendor charges $1200 per year for certification testing for a single system set, plus $400 for each additional system. Make sure costing includes time for testing with clearinghouses and any major payers.

----
* Business Process Reengineering:

While it can be difficult to estimate related costs, this should be one of your strongest money-saving HIPAA initiatives. Major steps include documenting and analyzing existing processes, process reengineering, and implementation. Primary cost drivers: total number of processes evaluated, consulting assistance (if needed), and documentation and training time.

----
* Technical Security Program:

Major elements include network and system technical assessment and responding to discovered weaknesses, representing most of the product purchase costs you will incur. Firewall costs range from $10,000 to $40,000, with initial training costs of $3000 to $7000. Don't forget maintenance: an average of 2.5 hours per day or (loaded cost) $20,000 per year. Intrusion detection costs range from $10,000 to $50,000 plus installation, with staff support ranging from $25,000 to $50,000, and 24 X 7 monitoring costing $20,000 to $28,000 per year. Savings of 50-60% are possible through outsourcing.

----
* IT Configuration Management:

Covers controls put into place to prevent user adaptations to standard system configurations (including individual workstations) that might affect your organization's security. Major cost items include staff time, application software control and version changes, automated network management systems, hardware inventory control, OS and network upgrades supporting "minimum necessary" restrictions, and strengthened virus protection. The major cost driver is the number of computers that must be managed, and the time needed for hands-on management for each. Larger organizations may need to utilize (and pay for) automated tools to minimize man hours.

----
* Physical Security:

Major cost drivers are employment of a Security Officer, purchases of shredding devices and other physical security devices such as electronic locks and closed circuit TV, and time and purchases related to contingency/disaster recovery planning. In a large organization, total security staff should be 1 FTE per 1000-1500 users; consider .1 FTE for up to 50 users. Physical security devices can be estimated at $5000-$25,000 for most facilities -- but recognize that items such as electronic locks cost about $3000 (installed) per door. Costs for contingency and disaster recovery depend entirely on your organization's current status and its risk tolerance levels; a key cost decision will be hot-site vs. cold-site vs. backups only solutions. Outside assistance on a new plan will range from $50,000 to $100,000.

----
* Privacy Program:

Major elements include employing a Privacy Officer, and development, coordination and implementation hours for setting up patients' rights processes, and for development and implementation of Privacy policies, procedures and processes. The Privacy Officer will be a full-time job in large organizations, but an add-on in smaller facilities. Costing should consider that setting up policies and procedures will require up to 250 person days in large organizations, and as much as half that time in smaller facilities. Applying quality, externally-procured policy templates will help eliminate policy development time by approximately 60 days of time, but do not discount the time needed to customize them to your environment.

----
* Training:

Budgeting should capture general awareness, and Privacy/Security training for workforce members, including health information management changes, development of new employee and refresher programs and computer system training necessitated by Transactions-related upgrades. Major cost drivers include staff hours to develop, coordinate, implement and attend training sessions. Costs of outside expertise and delivery methods should be included, and, if appropriate, the time/costs for adapting externally developed materials.

----
* Business Associates:

Tasks include developing your business associate database, drafting and coordinating agreements, and implementing process changes. Major cost drivers include number of business associates, legal review of agreements, implementation labor hours, and hours for maintenance, renewal, and enforcement of agreements.

THE DEVIL IS IN THE DATA ANALYSIS:

With all estimates in hand, you should be able to finalize a budget after completing these last steps in the costing process:

1. Revisit and re-evaluate assumptions relative to your environment.
2. Review the remediation activities to determine if all apply, and to ascertain if others must be included.
3. Conduct a cost analysis. Are your cost estimates within the suggested ranges? If not, is there a justifiable reason why not?
4. Is the total cost too high? If so, review HIPAA directives regarding solution scalability and reasonableness. Re-evaluate risk tolerance levels, consider lower-cost technology options, reconsider level of reliance on external resources, and (conversely) consider outsourcing options.
5. Create a time schedule for remediation that meets HIPAA requirements and your staffing/purchasing capabilities.
6. Finalize cost estimates.
7. Finally, document the costing process.

Article excerpted from Health Management Technology, October 2002

D'Arcy Guerin Gue is Executive Vice President, Knowledge Services and Business Development, Phoenix Health Systems, Inc. This article was co-authored by John Spearly, Executive Vice President, and Tom Grove, Vice President, Phoenix Health Systems. Phoenix is expert in HIPAA change management, strategic planning, and procurement, implementation and integration of state-of-the-art health care information technology.

==

4 >> H I P A A / SECURE: Guest Article

** Finding HIPAA Compliant Solutions for Data Backup and Recovery **

By Jenny Pemberton

The need to become HIPAA compliant is driving physicians to examine every process and system in their offices. Backing up data has become a high priority as a result of the HIPAA security requirements not only for backing up and protecting data, but being able to document the entire process.

There are a number of methods for backing up data, each with its advantages and disadvantages. As in all technology, more secure and automated processes continue to evolve.

Years ago, backing up to floppy disks was a widely acceptable practice. But doctors soon learned that the disks cannot hold enough memory for unattended backups. Each backup could require hundreds of disks and storage is unreliable.

Today, the most widely-used method for backing up data is the traditional tape backup. Tapes provide a relatively high storage capacity and eliminate the need to sit and watch the backup and change storage acceptance devices. However, the higher quality comes at a higher price. Getting started requires an average initial investment of around $2,000 to purchase the drive and the backup software. Then, a rotating backup routine recommends using 19 tapes per year at an average cost of $40 a tape. Often, a practice will just tape over and over on the same tape only to discover that it has worn out and the last recognizable backup may be a year old. Tape backups also require an off-site storage solution -- where to keep the tapes in the event of a data loss, system crash or even greater disaster? A practice must address how quickly those tapes can be retrieved and the data restored in such an emergency.

Some practices have tried removable storage drives -- though this is not very common. While a large floppy-disk drive or removable hard-disk equivalent drive are better than nothing, they are not highly recommended because of high pricing, cumbersome off-site storage issues and storage capacity limitations that make unattended backups impractical.

One method of backup that has become more popular is a CD backup. CD formats include recordable (CD-R) and rewriteable (CD-RW). Recordable CDs, once recorded, cannot be written over and can be read from any CD-ROM drive. Rewriteable CDs can be rewritten, but can only be read by the newer CD-ROM drives. This method of backing up is fairly inexpensive as the price of CDs continues to drop. But CDs don't hold as much storage capacity as a tape backup method. DVDs, an upgrade to CDs, hold up to 18 gigs of data. But with CD or DVD, the issues of off-site storage and limited shelf-life remain.

A new solution to providing both high quality security and off-site storage has evolved with the growing access to communications bandwidth -- online data backup. The online backup service is completely automated. The software is installed on the PC or server and compresses and encrypts the data prior to transferring it to a Data Center via a direct port. The backup occurs at night, the data is safely stored off-site in its encrypted format and it can be restored at the push of a button in the event of a disaster. The backup software has a selection feature that allows the customer to decide which files to be backed up, enabling cost-effective selection of data files only. And the backup success is monitored by data center experts. Typically, there are no upfront costs for the software and many services offer a free 30-day trial. Monthly pricing is based on the amount of compressed data stored on the provider's servers and is typically less expensive than the cost of tapes. For example, a typical two-physician practice using practice management software on a Windows-based operating system might have 50 - 200 megs of compressed data. In such a case, the monthly online backup cost would range from $20 to $40.

With HIPAA compliance deadlines looming, physicians must evaluate their backup process and make plans to write a contingency plan. This plan should include information about how the backup process is done, who handles the tapes or CDs, where they are stored off-site, how quickly they can be retrieved in the event of a disaster, the rotation process -- everything related to backing up the data, protecting it, storing it and recovering it. There are backup services that have geared their company structure to meet the stringent requirements of HIPAA and will even provide a written contingency plan free as part of their backup process. Practices that haven't just purchased tape drives or expensive equipment would do well to consider looking into online backup solutions.

Jenny Pemberton is Business Development Director for DataHEALTH, of Ashland, KY. DataHEALTH provides online data backup and disaster recovery solutions to the health care industry,serving customers in nine countries.

===

5 >> HIPAA / SECURE: Security Q/A

** Security Solutions: Key Technologies and Practices **
>> Access Control <<

By Eric Maiwald, CISSP

QUESTION: Can you explain what access control is and how it will be needed to protect PHI?

ANSWER: Access control is simply limiting who can see what information. The draft security rule requires that access to PHI be limited to only those individuals who require access to the information. Given this requirement it is important to have an understanding of what job functions will require access to what information and then to make sure that access to information is limited accordingly.

There are two primary types of access control: Role-based and Identity-based. Role-based access control (RBAC) bases the decision to allow access to information or not on the job the individual is performing. For example, the job of "nurse" may require access to a patient's medical history. This may include information on allergies, current illnesses, and past surgeries. Thus when a nurse requests this information, the system grants the request. Another job such as "billing clerk" may only require access to the patient's account. Thus a request by the clerk for information on allergies would not be allowed. In order for RBAC to function properly, the organization must identify which information is necessary for each role or job. Then as users are added to the system, they must also be grouped into the various roles.

An alternative to RBAC is identity-based access control (IBAC). IBAC uses the identity of the individual to make access control decisions rather than the role that the individual is playing in the organization. In this case, the organization would define what files or information "John" had access to. If John attempted to access information that he is authorized to access, the system would allow the access. If not, the system would deny the access attempt. The organization would need to establish the access control rules for each user in the system.

Be aware that access control rules can get very specific. For example, it may be necessary to allow nurses in the emergency room to have access to information about emergency room patients. However, until the patient is admitted to a service in the hospital, no other nurse is allowed to see the patient's information.

The actual establishment of an appropriate access control policy will take some thought. Make sure that the policy takes into account all of the various job functions and how the individuals in those jobs do their jobs. It is very easy with access control to make people's jobs very difficult.

Eric Maiwald, CISSP, is Chief Technology Officer of Fortrex Technologies, which provides information security management, and process and monitoring services for healthcare organizations and other industries.

==

6 >> HIPAA / LAW: Legal Q/A

** Do Assisted Living Facilities Qualify as Covered Entities? **

By Steve Fox & Rachel Wilson, Esqs.

QUESTION: Are Assisted Living Facilities covered under the HIPAA regulations?

ANSWER: It depends upon the circumstances, as is so often the case with HIPAA. Assisted living facilities can vary widely in their billing practices and in the array of services they provide. Such facilities do not qualify as "health care clearinghouses" and are not likely to fall under the definition of a "health plan" under HIPAA. However, an assisted living facility may engage in certain activities or functions sufficient to qualify as a "health care provider," subject to regulation under HIPAA.

"Assisted Living Facility" is a generic term used to describe facilities that bridge the gap, primarily, though not exclusively, for senior citizens, between independent living and residence in nursing homes. The term refers to many different types of care arrangements including help with meal preparation, bathing, dressing, performing household chores, and in many instances, providing some form of medical care. Certain of these facilities may be eligible for Medicaid reimbursement while others are not. Assisted living facilities may be part of a retirement community, nursing home or elder-housing facility or they may stand alone.

Regardless of the title or structure, the status of any assisted care facility as an entity subject to HIPAA regulation can be determined by utilizing a three-part analysis.

1. First, does the facility furnish, bill, or receive payment for health care in the normal course of business?

-- "Health care" is defined as care, services, or supplies related to the health of an individual. It includes, but is not limited to, preventive, diagnostic, rehabilitative, or maintenance care, counseling, or assessment services with respect to the physical or mental condition of an individual as well as the sale or dispensing of a drug in accordance with a prescription.

2. Second, does the facility conduct covered transactions?

-- A "covered transaction" is the transmission of information to carry out certain administrative and financial activities including, but not limited to, health care claims or equivalent encounter information and coordination of benefits. If an assisted living facility uses another entity to conduct covered transactions on its behalf, the facility is treated no differently than if it conducted the transactions directly as opposed to conducting them indirectly through an intermediary.

3. Finally, are any of the covered transactions conducted in electronic form?

-- Covered transactions conducted by transmitting information over the Internet, an Extranet, leased lines, dial-up lines, private networks, as well as those transmissions that are physically moved from one location to another using magnetic tape, disk or CD media all qualify.

If the answer to all three of the preceding questions is "yes," then the assisted care facility is a "health care provider" as defined under HIPAA.

For further reference, a decision tree of this analysis, along with other decision trees regarding qualification as a "health care clearinghouse" or "health plan" under HIPAA, is posted on the Center for Medicare and Medicaid Services' web site and can be found at: http://www.cms.gov/hipaa/hipaa2/support/tools/decisionsupport/default.asp.

Read past HIPAA Legal Q/A articles:
http://www.hipaadvisory.com/action/LegalQA/archives.htm

Steve Fox, Esq., is a partner at the Washington, DC office of Pepper Hamilton LLP. This article was co-authored by Rachel H. Wilson, Esq., of Pepper Hamilton.
DISCLAIMER: This information is general in nature and should not be relied upon as legal advice.

==

COMMENTS? Email us at info@phoenixhealth.com
SUBSCRIBE? Visit http://www.hipaalert.com
ARCHIVES: http://www.hipaadvisory.com/alert/archives.htm

==

==

You are currently subscribed to hipaalert as: kmckinst@dmhhq.state.ca.us

To UNSUBSCRIBE, send an email to: leave-hipaalert-8507990O@lists.hipaalert.com